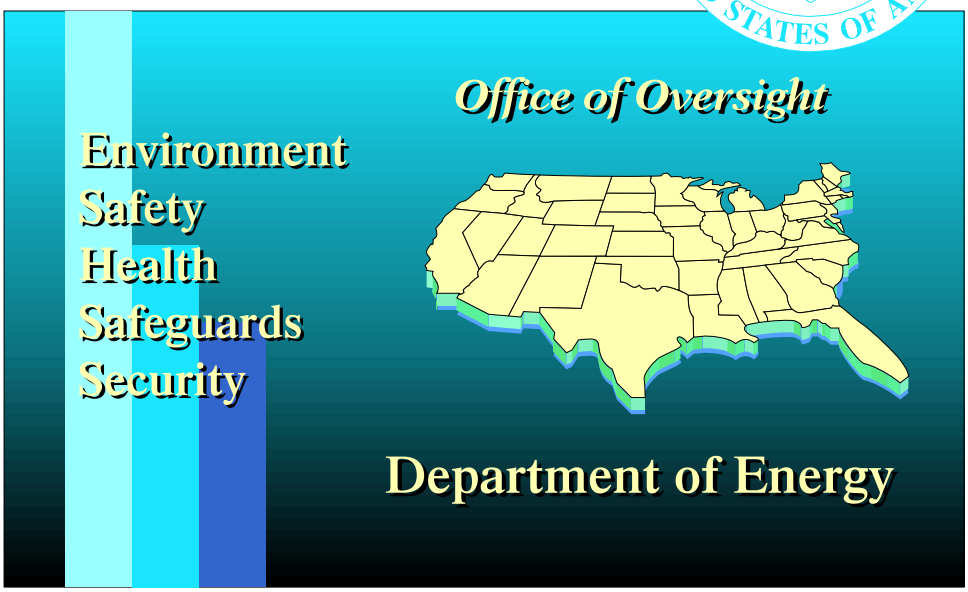
EH2PUB/05-97/04SE

OVERSIGHT

Lawrence Livermore National Laboratory

Safeguards and Security Profile Summary Analysis

May 1997



Office of Environment, Safety and Health

1.0 Introduction

The Department of Energy (DOE), Office of Environment, Safety and Health, conducted a review in May 1997 to determine the status of safeguards and security at the Lawrence Livermore National Laboratory. This review was part of a recent initiative by the Assistant Secretary for Environment, Safety and Health to characterize the current status of safeguards and security programs throughout the Department. The Assistant Secretary for Environment, Safety and Health utilizes the Office of Oversight to provide the Secretary of Energy with independent assessments of the Department's performance in the areas of environmental protection, safety, health, and security. This document describes significant aspects of the safeguards and security posture at the Lawrence Livermore National Laboratory observed during the review.

2.0 Background

Location

Lawrence Livermore National Laboratory occupies 821 acres near the city of Livermore, California, approximately 45 miles east of San Francisco. The main laboratory facilities are located on flat terrain on the eastern border of the city of Livermore. Site 300 (an explosives test area) is located on approximately 11 square miles in rolling hills 17 miles southeast of the main laboratory.

Mission

The current mission of the Laboratory is to solve complex scientific and technical problems of national importance. The hallmark of the Laboratory is its ability to translate basic science concepts into technologies that solve complicated real-world problems and expand the boundaries of fundamental science.

Security Assets/Interests

The Laboratory possesses 4,300 plutonium and enriched uranium items in the form of metals, weapons parts, complete weapons assemblies, oxides, and waste, some of which are considered by DOE as potential radiological sabotage targets. Classified holdings consist of the equivalent of over two million documents, mainly in 1,400 classified computer systems, and including over 800,000 documents and items, including 3,200 non-nuclear weapons parts and tooling.

Protection Strategy

The Lawrence Livermore National Laboratory site employs a multiple-layered protection strategy. These layers include: (1) physical barriers (fences, barbed wire, razor ribbon) and electronic intrusion detection systems at the exterior boundaries of site security areas; (2) the buildings in which the assets are located and the intrusion detection systems, alarms, access controls, and search procedures associated with those buildings; and (3) the vaults, vault-type rooms, safes, and associated intrusion

detection systems and administrative controls within those buildings in which the assets are stored.

There are a number of administrative and electronic or mechanical protection measures employed at various points throughout the layers of protection. Administrative measures include the security clearances granted to personnel having access to various security interests, a human reliability program that employs random drug and alcohol tests and psychological testing for personnel with direct access to certain types and quantities of nuclear materials, a staff badging system to distinguish staff with security clearances from those without, numerous entry/exit points staffed by protective force personnel, and protocols such as "two person" rules which assure that at least two personnel are present when nuclear material is being handled in order to minimize the possibility that a single insider could commit a malevolent act undetected. Electronic/mechanical protection measures include various access controls such as cipher locks, magnetic key cards and personal identification numbers, closed circuit television, and an array of safe combination locks and lock and key controls. The Laboratory also has a protective force that assesses and responds to security matters on site.

3.0 Results of Past Safeguards and Security Reviews

The most recent safeguards and security review by the Office of Security Evaluations, in 1994, revealed generally effective protective force and physical security system programs, with only isolated deficiencies. The Laboratory's human reliability program was found to be less than optimally effective, and the need to sharply reduce the large number of security clearances was noted. Problems in quantifying nuclear material holdings and verifying accountability of nuclear materials during inventories were also observed. Finally, in protection of classified information, one aspect of the Laboratory's implementation of "need-to-know" was inconsistent with DOE policy, and the computer security program suffered from problems in computer system accreditation, certification, and configuration management.

4.0 Results of This Review

Positive Trends and Initiatives

Since the 1994 inspection by the Office of Security Evaluations, Lawrence Livermore National Laboratory has made progress in addressing most of the concerns identified at that time. Both the classified and unclassified computer security programs (designed to protect classified and unclassified sensitive information stored on computer systems) have improved and show positive indications of management emphasis and support. The Laboratory has implemented a formal process to ensure that computer security concerns, issues, and requirements are sufficiently addressed before projects involving computer assets proceed.

The personnel security program, which ensures the reliability of individuals having access to nuclear material and classified information, has also been improved. Security clearance reduction efforts over the past three years have resulted in a 28 percent decrease in the number of Laboratory staff with security clearances. Likewise, the site's program for controlling, inventorying, measuring, and formally accounting for nuclear material has been enhanced. The procurement and use of better measurement equipment has improved the Laboratory's ability to measure nuclear materials accurately.

Although concerns identified during the 1994 inspection have been addressed, as discussed below, recent performance tests indicated that protection of special nuclear material has degraded in the past two years, most notably by the reductions in protective force capabilities (e.g., reduction in protective force personnel stationed at the area where most Laboratory special nuclear material is used and stored, and the elimination of the special response team). The Laboratory has provided temporary security measures to improve the protective posture while permanent changes are made. Further, the Laboratory has been innovative in devising ways to rapidly install some of the needed improvements. Although some actions have been taken to date, concerns over the effectiveness of the current protection system remain.

Safeguards and Security Concerns

The "Openness" Initiative versus Protection Program Effectiveness

During the 1990s, at the direction of DOE, the Laboratory has steadily reduced its investment in protection. The Laboratory has been opened to public access in many areas, and access restrictions have been reduced in many others. Protective force staffing in areas where nuclear materials are used and stored was cut almost in half. These trends supported the Department's openness initiative, reduced Laboratory indirect costs, and provided a more open working environment for Laboratory staff. DOE managers at the local and Headquarters levels approved each reduction. However, a series of performance tests conducted in the summer of 1996 revealed that these initiatives had been taken too far, leading to a serious reduction in overall program effectiveness.

Previous imperatives to reduce security expenditures, including a performance objective in the University of California's contract (which provides salary increases for senior managers based on reducing safeguards and security costs), still remain; however, they are somewhat tempered by the recent revelation of concerns. A significant level of management attention will be required to maintain an appropriate balance between the need to reduce costs and increase openness on the one hand, and the need for effective security on the other.

Effectiveness of Interim Protection Measures

Immediately following the series of performance tests conducted in the summer of 1996 that revealed vulnerabilities in the Laboratory's protection system, interim compensatory measures were implemented to enhance the Laboratory's security posture while permanent upgrades were planned and completed. Compensatory measures included establishing additional protective force posts and strengthening access control procedures. These interim measures will remain in effect until all permanent upgrades are complete.

After these performance tests, the DOE Oakland Operations Office directed the Laboratory to thoroughly analyze the lessons learned. Their analysis identified additional concerns in areas such as access controls and search procedures, leading to some immediate changes and the identification of others that will require more time to complete. During the next year, detection systems will be upgraded and enhanced, and the Laboratory will re-establish a special response team to enhance their capability to respond quickly and effectively to security threats.

The status of both interim compensatory measures and permanent upgrades must be monitored closely by the Department until effective levels of performance have been performance tested, analyzed, and validated. Additionally, overall improved internal and external communications on security matters are needed. DOE Headquarters has not effectively formulated and communicated its expectations to the Oakland Operations Office and the Laboratory. However, there continues to be effective communication between the Laboratory and the Operations Office concerning the consequences of protection failure and the resources to provide sufficient protection. Continued and open communication between Headquarters, the Operations Office, and the Laboratory is essential to complete the upgrades that will enhance the security posture at the Laboratory.

Consistent Application of Protection for All Information Security Assets

Classified matter protection and control at the Laboratory have greatly improved in recent years and are now generally at the level specified in DOE orders. Protection and control procedures are, for

the most part, appropriate and well implemented for much of the site. However, some areas of concern still remain which detract from this generally effective protection program. They concern the Laboratory's storage of some of its classified parts and tooling, its enforcement of need-to-know requirements, and its oversight of some restricted access programs. Additional protection emphasis by Laboratory management is needed in these three areas if the program is to demonstrate consistent application of its otherwise well-established controls for classified information.

Issues Warranting Management Attention

Continuing Ability to Conduct Clearance Investigations

There is currently a shortfall in funding for security clearance investigations. While the shortfall has not resulted in a noticeable adverse affect on the overall protection posture at the Laboratory, it may soon do so. If funding restrictions prevent or delay obtaining clearances for personnel to staff the special response team, plans for the team's deployment could be delayed. Moreover, an inability to conduct the required periodic clearance reinvestigations could reduce the effectiveness of the personnel security program in the overall protection posture. This situation merits close and continual monitoring by management.

Validation of Protection Against Radiological Sabotage

In the area of radiological sabotage, the Laboratory must assure that any adversaries attempting to gain access to a potential radiological sabotage target are denied such access, or the targets must be rapidly recaptured if denial fails. As the Laboratory finalizes the current draft site security plan, it should take care to include verification and validation of all potential targets on site and of the protective force's ability to deny adversary access and/or achieve timely recapture of these targets.